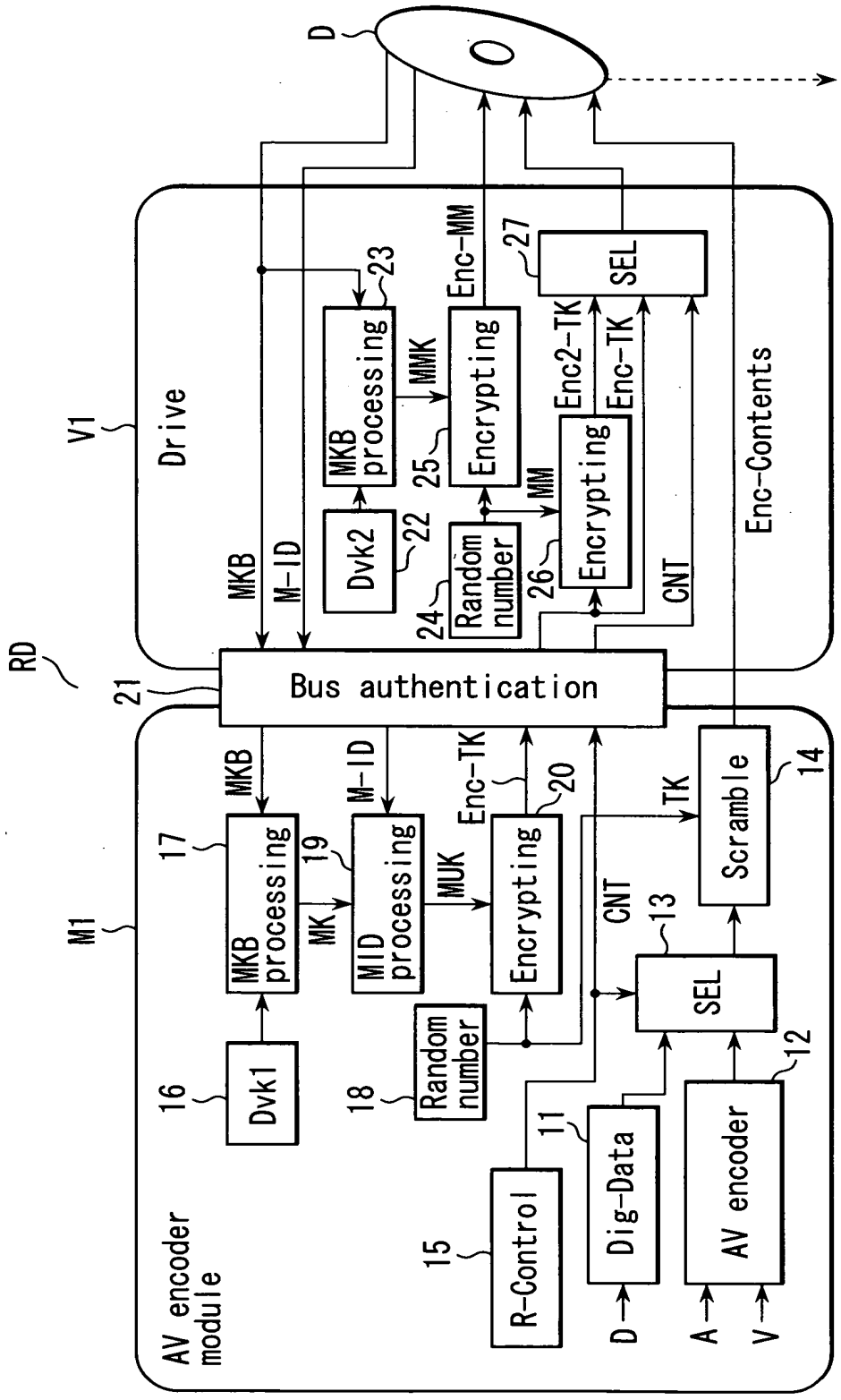
D
V1
Drive
MKB
M-ID
Dvk2
22
MKB processing
23
MMK
Encrypting
25
Enc-MM
27
SEL
Enc2-TK
Enc-TK
Encrypting
26
MM
Random number
24
CNT
Enc-Contents
RD
21
Bus authentication
M1
AV encoder module
MKB
17
MKB processing
MK
19
M-ID
MID processing
MUK
Enc-TK
Encrypting
20
TK
Scramble
14
CNT
13
SEL
16
Dvk1
18
Random number
11
Dig-Data
12
AV encoder
15
R-Control
D
A
V

FIG. 1

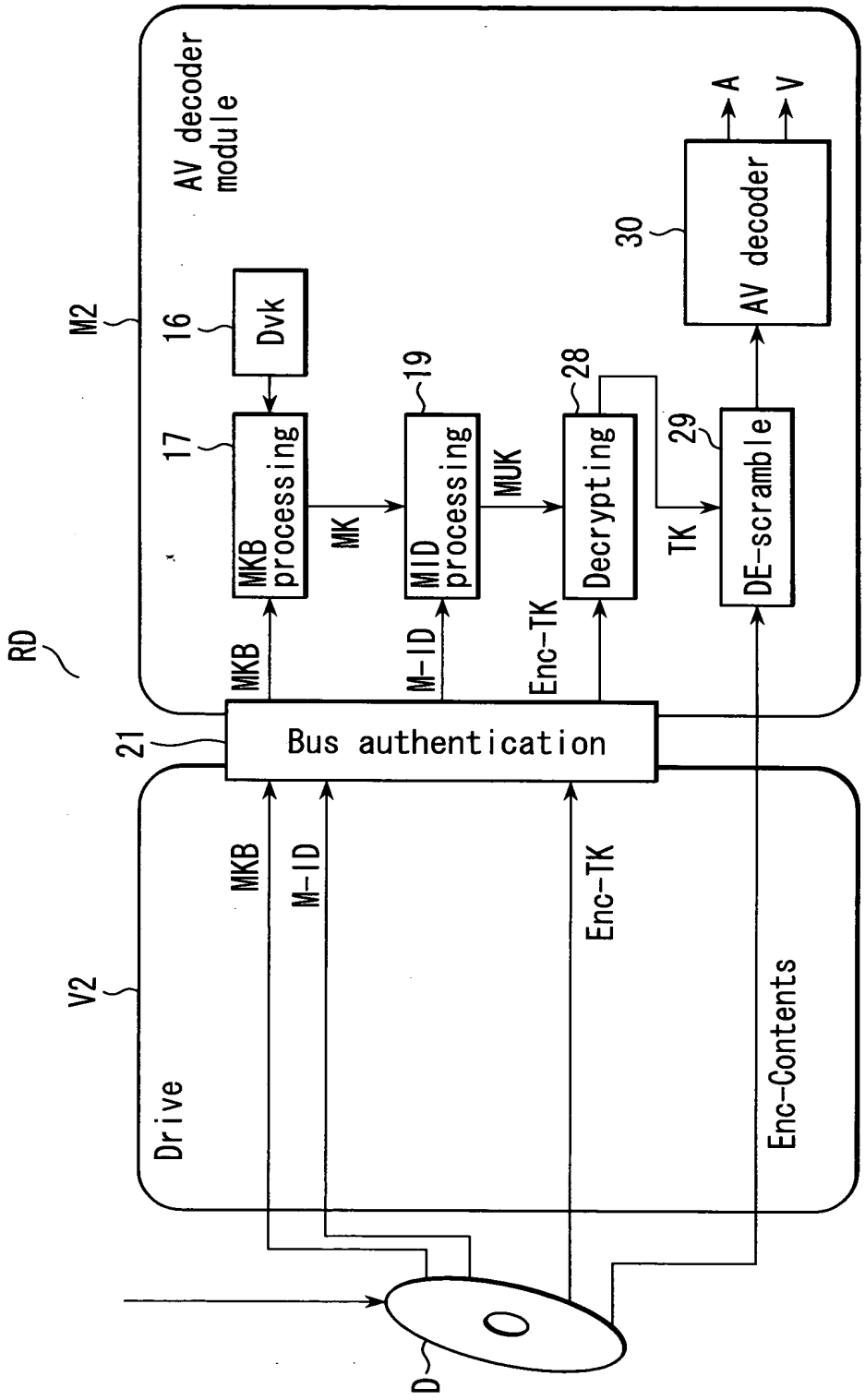
RD
M2
AV decoder module
16
Dvk
17
MKB processing
MK
19
MID processing
MUK
28
Decrypting
TK
29
DE-scramble
30
AV decoder
A
V
MKB
M-ID
Enc-TK
21
Bus authentication
V2
Drive
MKB
M-ID
Enc-TK
Enc-Contents
D

FIG. 2

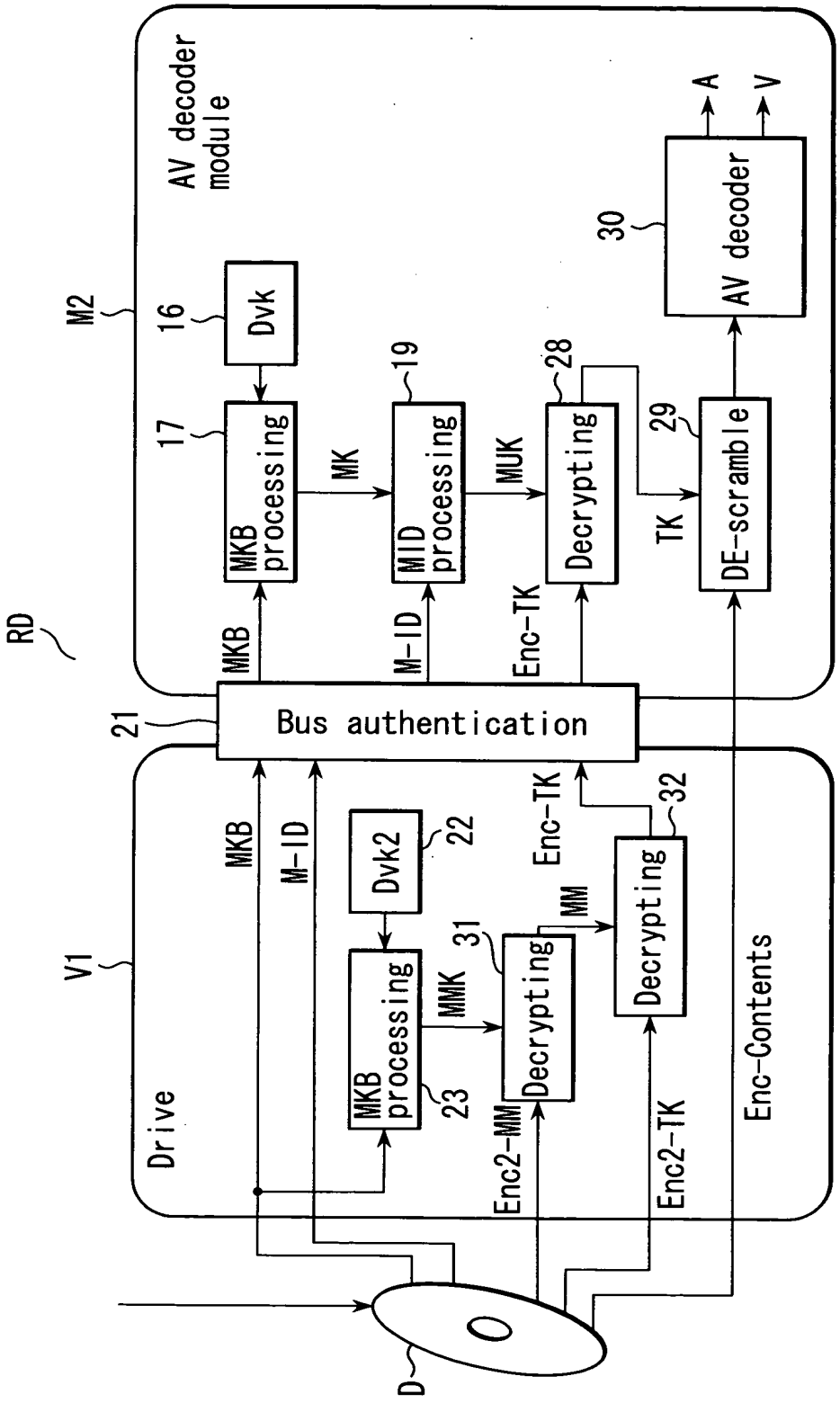
RD
AV decoder module
M2
16
Dvk
17
MKB processing
MK
19
MID processing
MUK
28
Decrypting
29
DE-scramble
TK
30
AV decoder
A
V
MKB
M-ID
Enc-TK
21
Bus authentication
V1
Drive
MKB
M-ID
Dvk2
22
MKB processing
23
MMK
31
Decrypting
Enc2-MM
MM
Enc-TK
32
Decrypting
Enc2-TK
Enc-Contents
D

FIG. 3

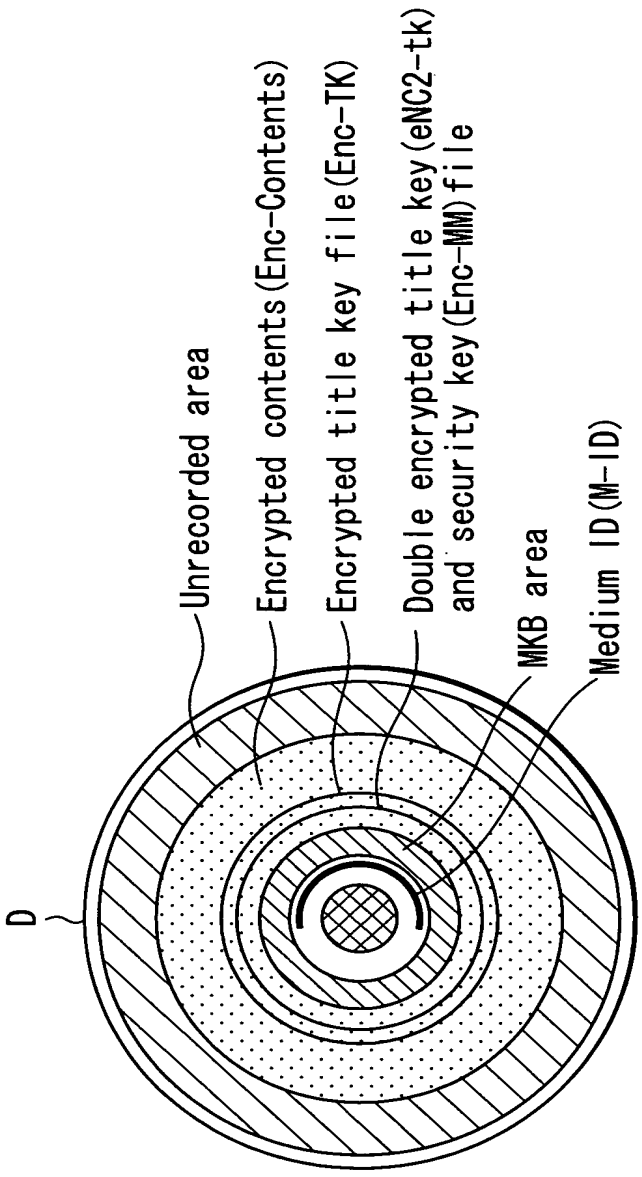
D
Unrecorded area
Encrypted contents (Enc-Contents)
Encrypted title key file (Enc-TK)
Double encrypted title key (eNC2-tk) and security key (Enc-MM) file
MKB area
Medium ID (M-ID)

FIG. 4

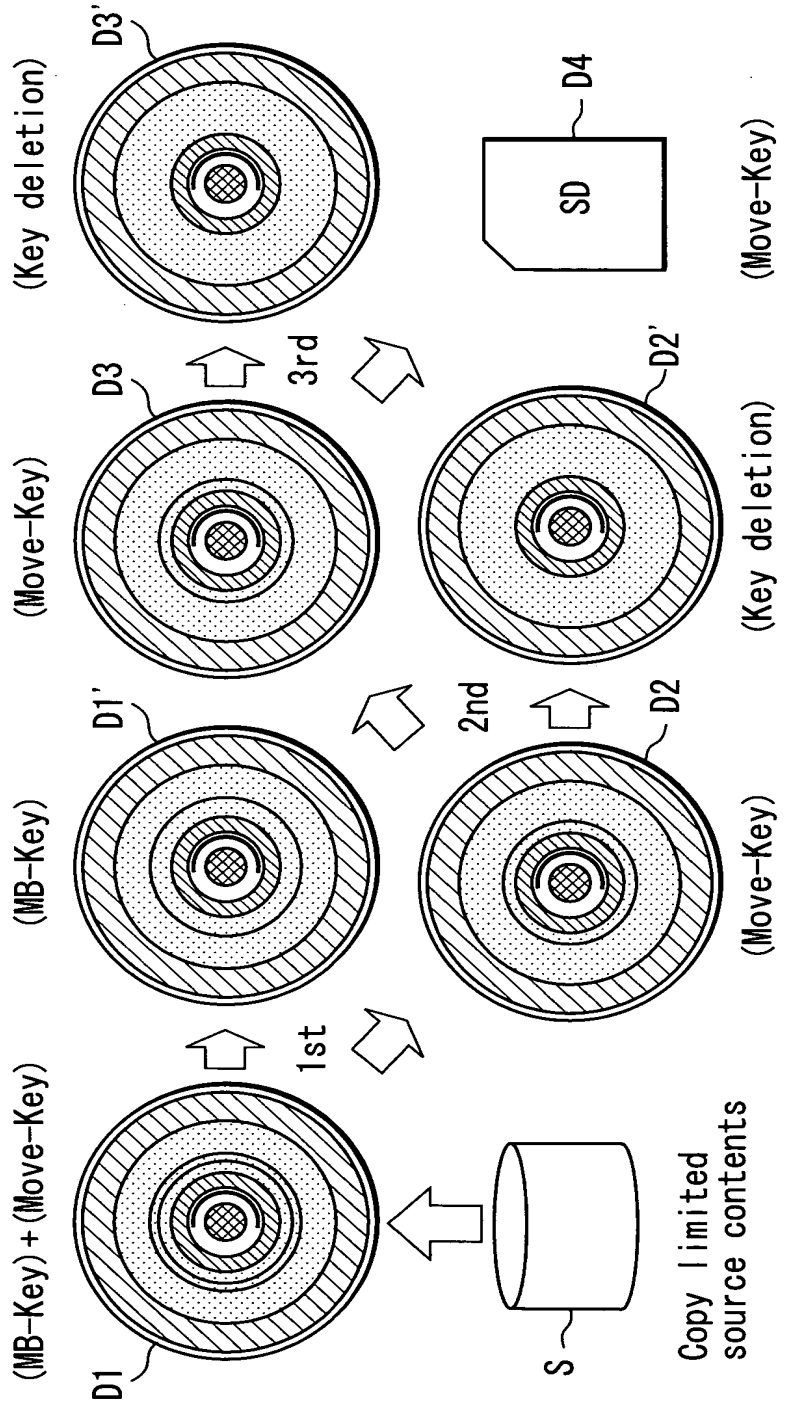
(MB-Key) + (Move-Key)
D1
1st
(MB-Key)
D1'
2nd
(Move-Key)
D2
(Move-Key)
D3
3rd
(Key deletion)
D3'
Copy limited
source contents
S
(Move-Key)
D2'
(Key deletion)
SD
D4

FIG. 5

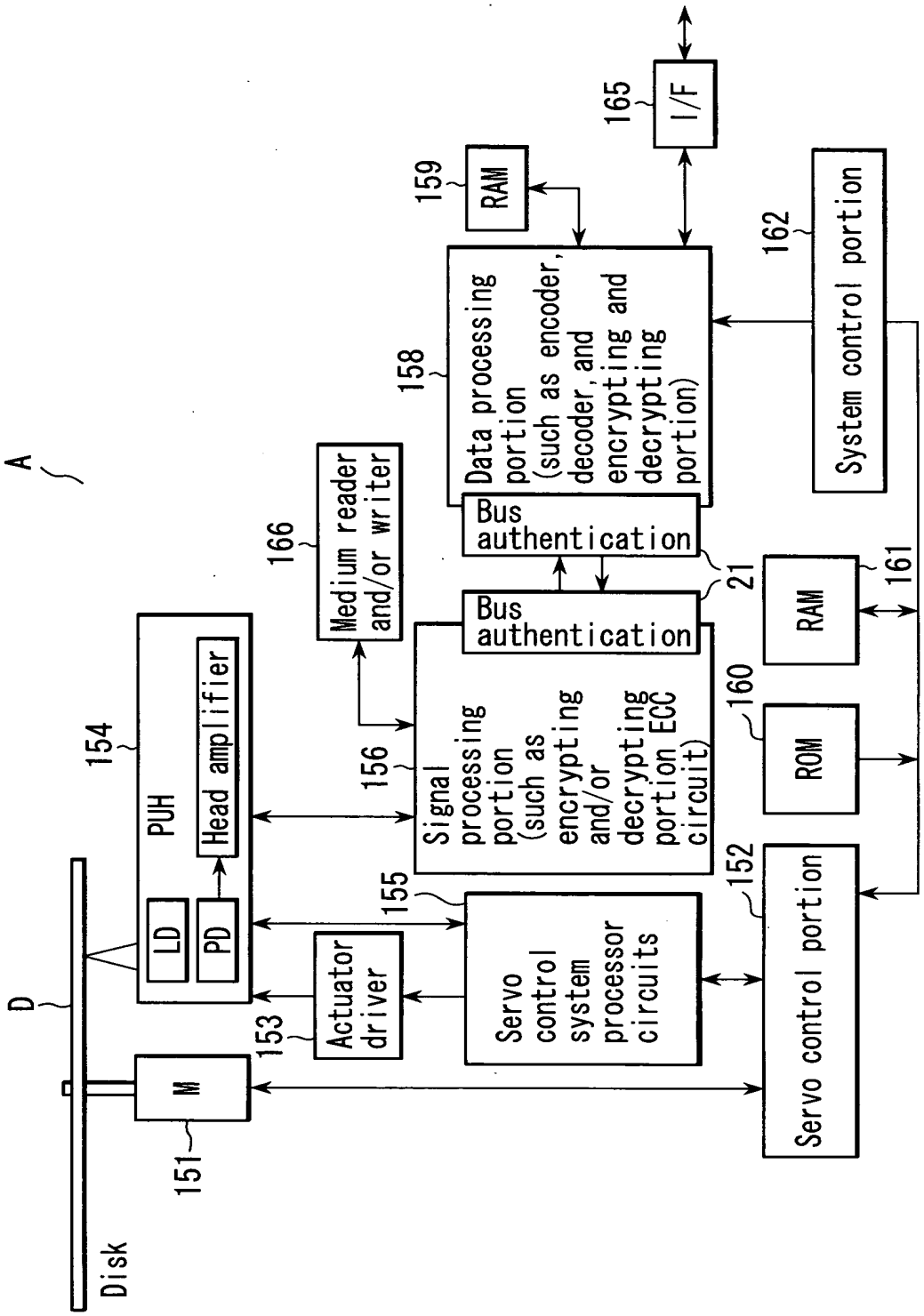
A
D
Disk
151
M
153
Actuator driver
154
PUH
Head amplifier
LD
PD
155
Servo control system processor circuits
156
Signal processing portion (such as encrypting and/or decrypting portion ECC circuit)
166
Medium reader and/or writer
158
Data processing portion (such as encoder, decoder, and encrypting and decrypting portion)
159
RAM
165
I/F
Bus authentication
Bus authentication
21
160
ROM
161
RAM
152
Servo control portion
162
System control portion

FIG. 6

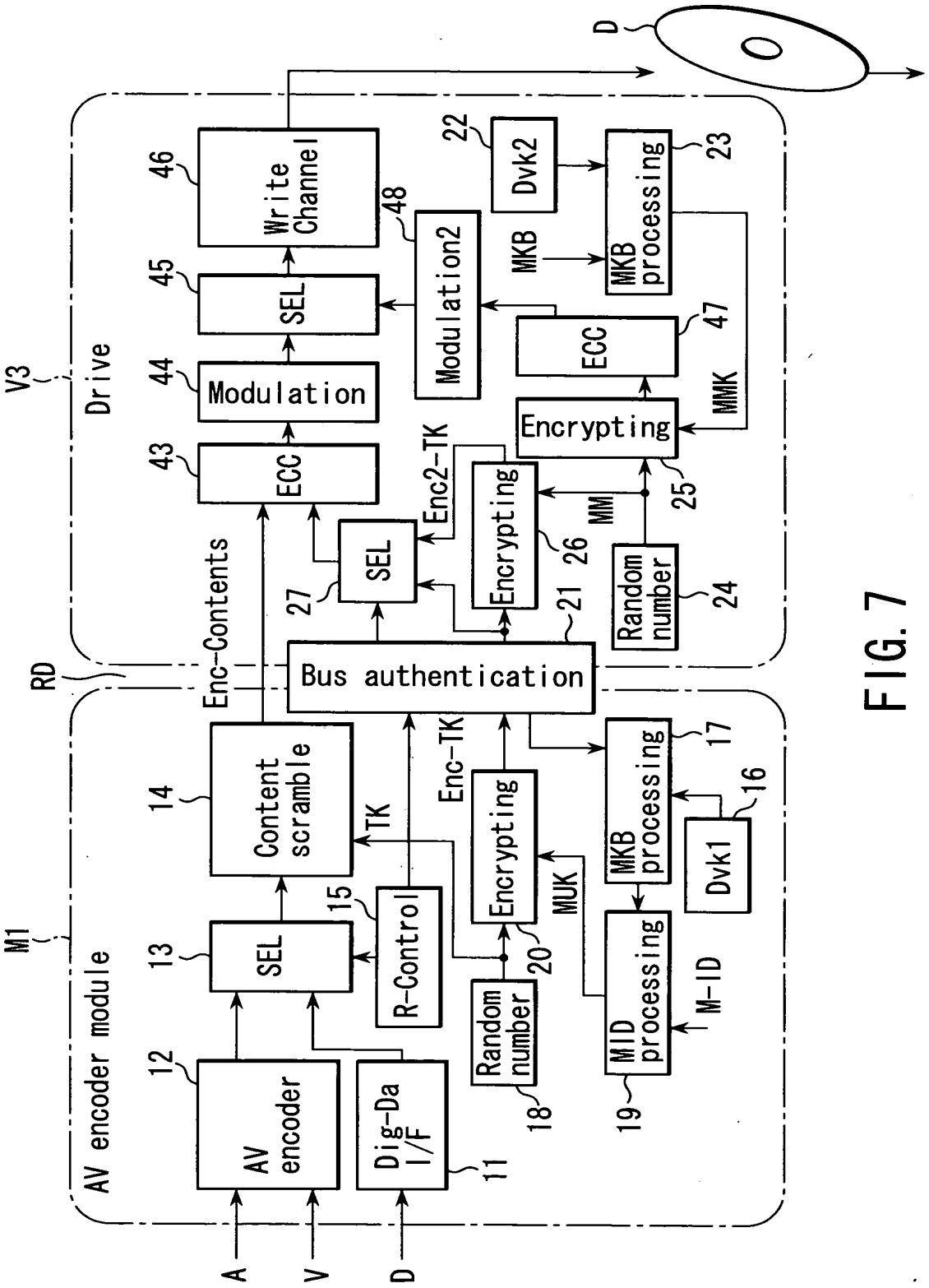
D
V3
Drive
RD
M1
AV encoder module
A
V
D
AV encoder
12
Dig-Da I/F
11
SEL
13
Content scramble
14
TK
R-Control
15
Random number
18
Encrypting
20
MUK
Enc-TK
Enc-Contents
Bus authentication
MID processing
19
M-ID
MKB processing
17
Dvk1
16
Random number
24
MM
Encrypting
26
Enc2-TK
SEL
27
21
ECC
43
Modulation
44
SEL
45
Write Channel
46
Encrypting
25
MMK
ECC
47
Modulation2
48
MKB
Dvk2
22
MKB processing
23

FIG. 7

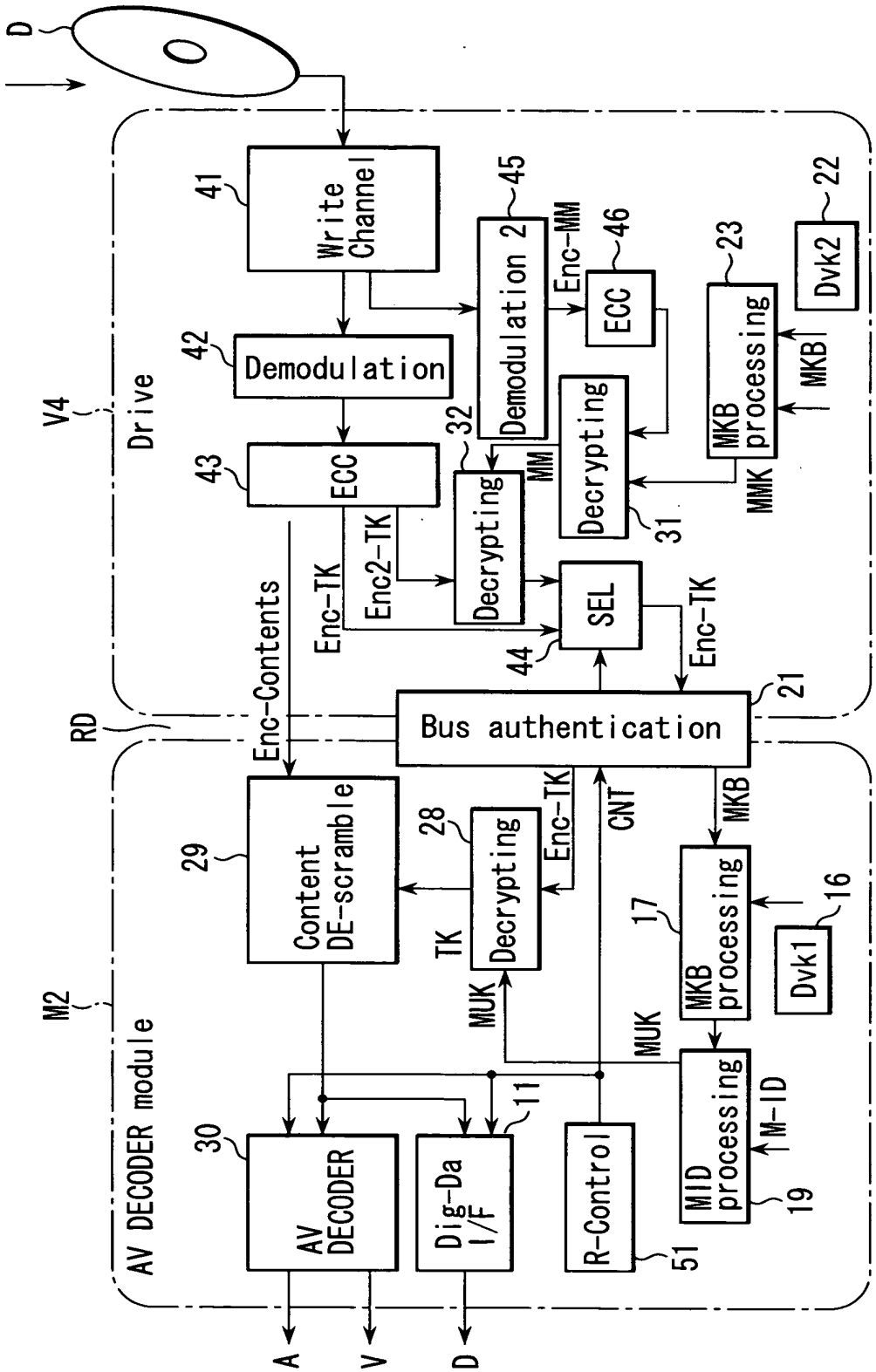
D
Drive
V4
41
Write Channel
42
Demodulation
43
ECC
32
Demodulation 2
45
Enc-MM
46
ECC
23
MKB processing
MKB
22
Dvk2
MM
MMK
Decrypting
31
Decrypting
Enc-TK
Enc2-TK
Enc-TK
SEL
44
Enc-TK
Enc-Contents
RD
Bus authentication
21
M2
AV DECODER module
29
Content DE-scramble
28
Decrypting
Enc-TK
TK
CNT
MKB
17
MKB processing
16
Dvk1
MUK
MUK
30
AV DECODER
11
Dig-Da I/F
R-Control
51
MID processing
M-ID
19
A
V
D

FIG. 8

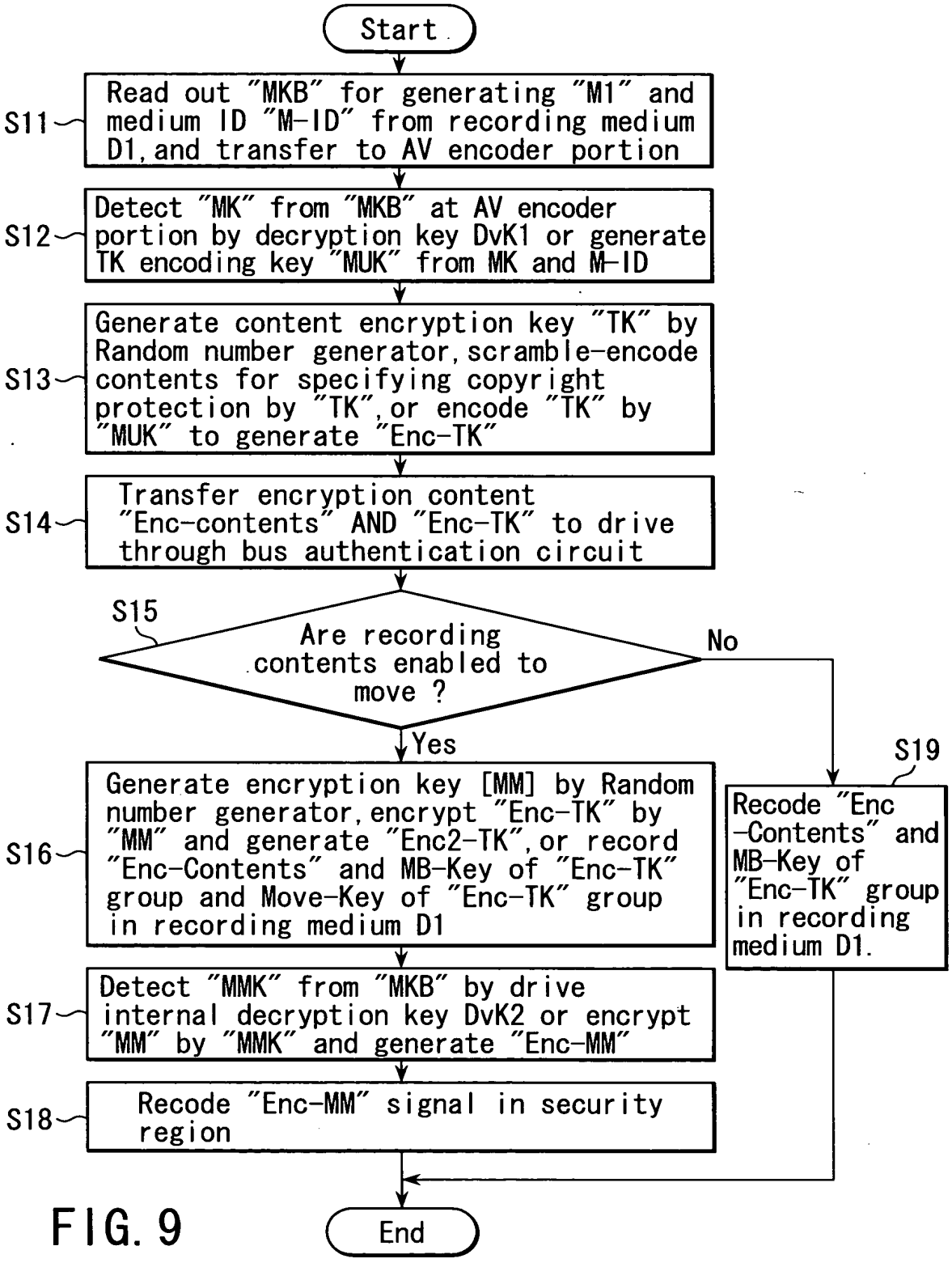
Start
S11
Read out "MKB" for generating "M1" and medium ID "M-ID" from recording medium D1, and transfer to AV encoder portion
S12
Detect "MK" from "MKB" at AV encoder portion by decryption key DvK1 or generate TK encoding key "MUK" from MK and M-ID
S13
Generate content encryption key "TK" by Random number generator, scramble-encode contents for specifying copyright protection by "TK", or encode "TK" by "MUK" to generate "Enc-TK"
S14
Transfer encryption content "Enc-contents" AND "Enc-TK" to drive through bus authentication circuit
S15
Are recording contents enabled to move ?
No
Yes
S16
Generate encryption key [MM] by Random number generator, encrypt "Enc-TK" by "MM" and generate "Enc2-TK", or record "Enc-Contents" and MB-Key of "Enc-TK" group and Move-Key of "Enc-TK" group in recording medium D1
S17
Detect "MMK" from "MKB" by drive internal decryption key DvK2 or encrypt "MM" by "MMK" and generate "Enc-MM"
S18
Recode "Enc-MM" signal in security region
S19
Recode "Enc-Contents" and MB-Key of "Enc-TK" group in recording medium D1.
End

FIG. 9

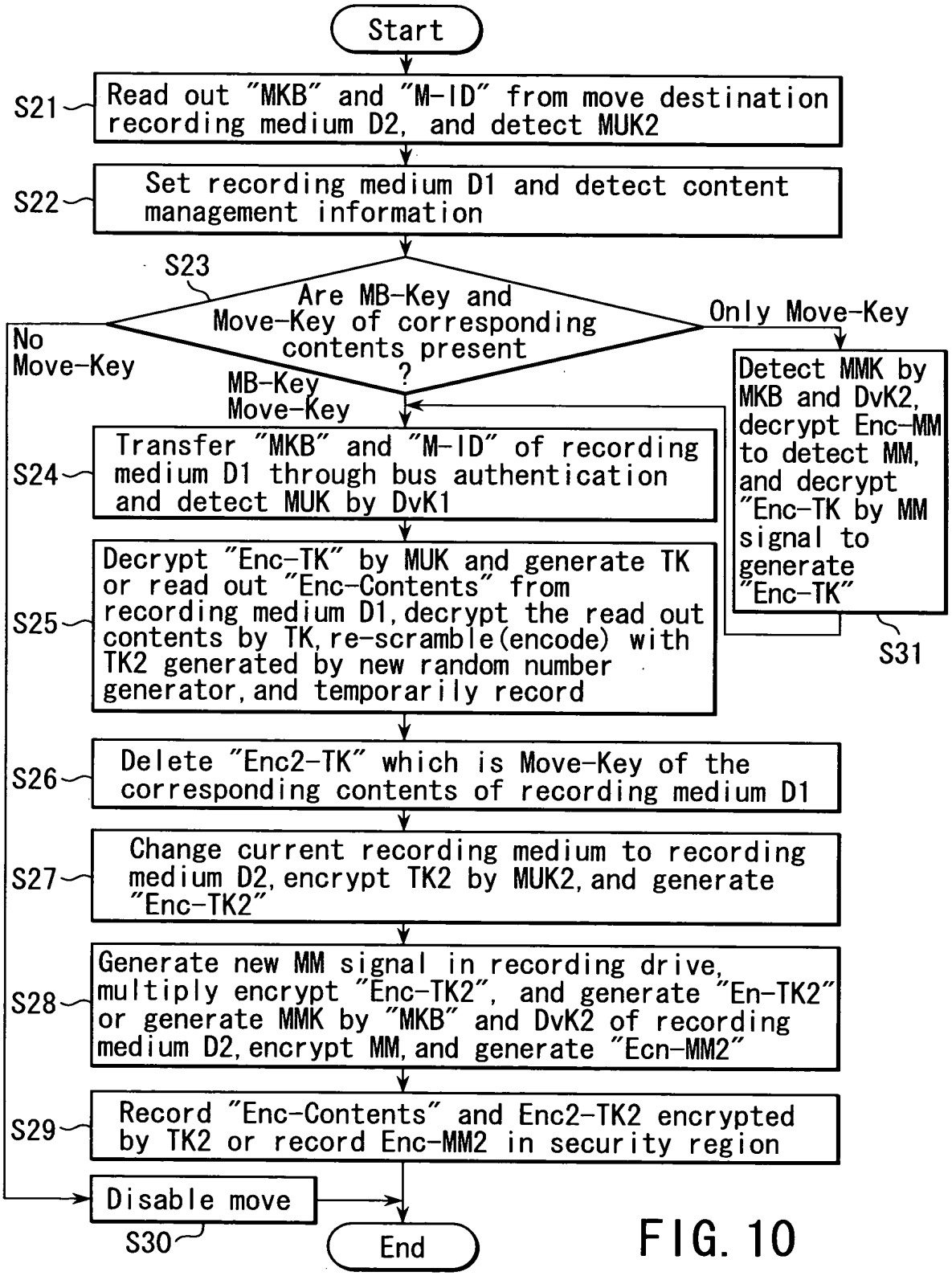
Start
S21
Read out "MKB" and "M-ID" from move destination recording medium D2, and detect MUK2
S22
Set recording medium D1 and detect content management information
S23
Are MB-Key and Move-Key of corresponding contents present ?
No Move-Key
Only Move-Key
MB-Key Move-Key
Detect MMK by MKB and DvK2, decrypt Enc-MM to detect MM, and decrypt "Enc-TK by MM signal to generate "Enc-TK"
S31
S24
Transfer "MKB" and "M-ID" of recording medium D1 through bus authentication and detect MUK by DvK1
S25
Decrypt "Enc-TK" by MUK and generate TK or read out "Enc-Contents" from recording medium D1, decrypt the read out contents by TK, re-scramble(encode) with TK2 generated by new random number generator, and temporarily record
S26
Delete "Enc2-TK" which is Move-Key of the corresponding contents of recording medium D1
S27
Change current recording medium to recording medium D2, encrypt TK2 by MUK2, and generate "Enc-TK2"
S28
Generate new MM signal in recording drive, multiply encrypt "Enc-TK2", and generate "En-TK2" or generate MMK by "MKB" and DvK2 of recording medium D2, encrypt MM, and generate "Ecn-MM2"
S29
Record "Enc-Contents" and Enc2-TK2 encrypted by TK2 or record Enc-MM2 in security region
Disable move
S30
End

FIG. 10

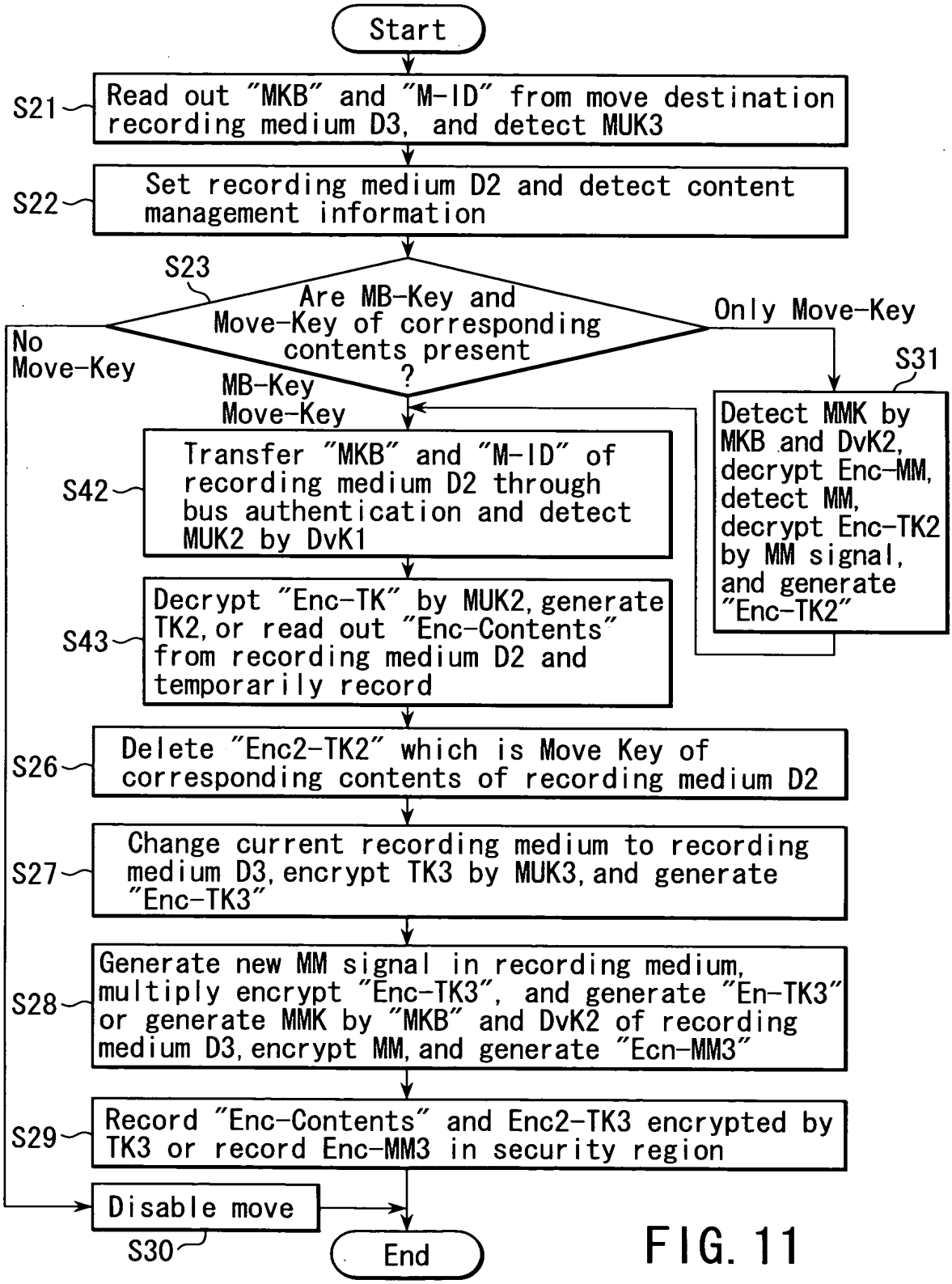
Start
S21
Read out "MKB" and "M-ID" from move destination recording medium D3, and detect MUK3
S22
Set recording medium D2 and detect content management information
S23
Are MB-Key and Move-Key of corresponding contents present ?
Only Move-Key
S31
Detect MMK by MKB and DvK2, decrypt Enc-MM, detect MM, decrypt Enc-TK2 by MM signal, and generate "Enc-TK2"
No Move-Key
MB-Key Move-Key
S42
Transfer "MKB" and "M-ID" of recording medium D2 through bus authentication and detect MUK2 by DvK1
S43
Decrypt "Enc-TK" by MUK2, generate TK2, or read out "Enc-Contents" from recording medium D2 and temporarily record
S26
Delete "Enc2-TK2" which is Move Key of corresponding contents of recording medium D2
S27
Change current recording medium to recording medium D3, encrypt TK3 by MUK3, and generate "Enc-TK3"
S28
Generate new MM signal in recording medium, multiply encrypt "Enc-TK3", and generate "En-TK3" or generate MMK by "MKB" and DvK2 of recording medium D3, encrypt MM, and generate "Ecn-MM3"
S29
Record "Enc-Contents" and Enc2-TK3 encrypted by TK3 or record Enc-MM3 in security region
Disable move
S30
End

FIG. 11

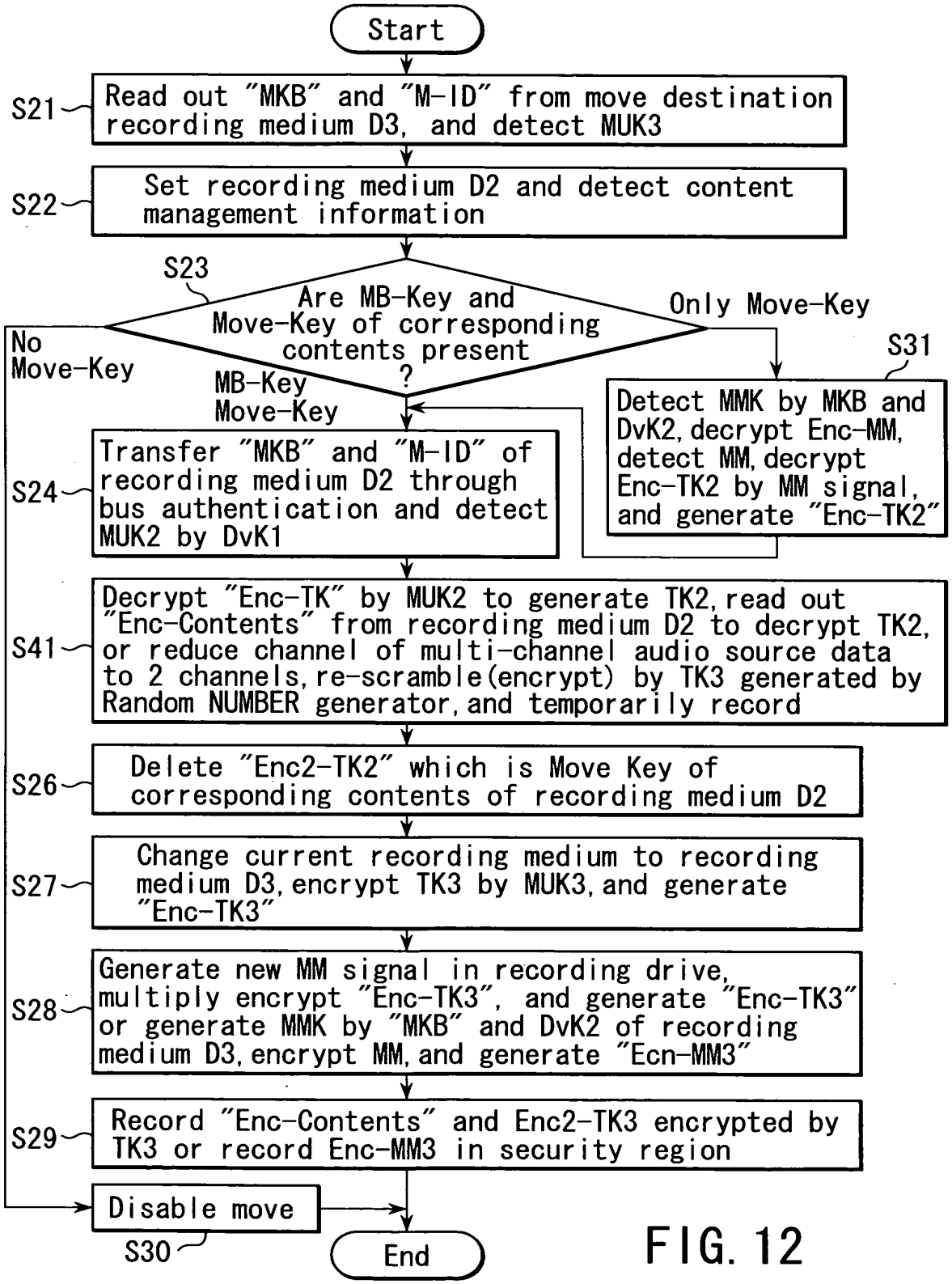
Start
S21
Read out "MKB" and "M-ID" from move destination recording medium D3, and detect MUK3
S22
Set recording medium D2 and detect content management information
S23
Are MB-Key and Move-Key of corresponding contents present ?
Only Move-Key
No Move-Key
MB-Key Move-Key
S31
Detect MMK by MKB and DvK2, decrypt Enc-MM, detect MM, decrypt Enc-TK2 by MM signal, and generate "Enc-TK2"
S24
Transfer "MKB" and "M-ID" of recording medium D2 through bus authentication and detect MUK2 by DvK1
S41
Decrypt "Enc-TK" by MUK2 to generate TK2, read out "Enc-Contents" from recording medium D2 to decrypt TK2, or reduce channel of multi-channel audio source data to 2 channels, re-scramble(encrypt) by TK3 generated by Random NUMBER generator, and temporarily record
S26
Delete "Enc2-TK2" which is Move Key of corresponding contents of recording medium D2
S27
Change current recording medium to recording medium D3, encrypt TK3 by MUK3, and generate "Enc-TK3"
S28
Generate new MM signal in recording drive, multiply encrypt "Enc-TK3", and generate "Enc-TK3" or generate MMK by "MKB" and DvK2 of recording medium D3, encrypt MM, and generate "Ecn-MM3"
S29
Record "Enc-Contents" and Enc2-TK3 encrypted by TK3 or record Enc-MM3 in security region
Disable move
S30
End

FIG. 12

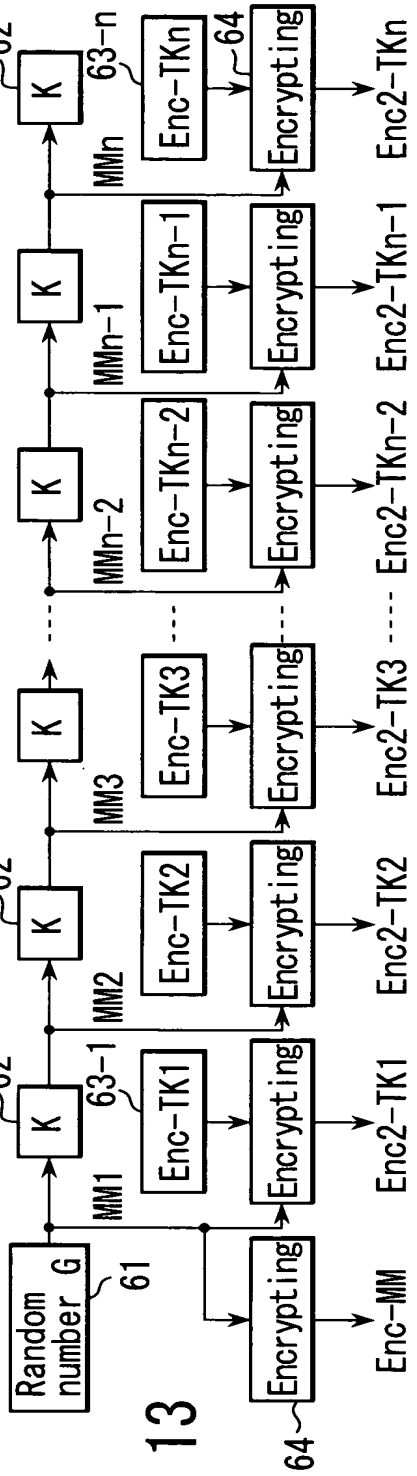
Random number G
61
62
K
MM1
MM2
MM3
MMn-2
MMn-1
MMn
63-1
63-n
Enc-TK1
Enc-TK2
Enc-TK3
Enc-TKn-2
Enc-TKn-1
Enc-TKn
64
Encrypting
Enc-MM
Enc2-TK1
Enc2-TK2
Enc2-TK3
Enc2-TKn-2
Enc2-TKn-1
Enc2-TKn

FIG. 13

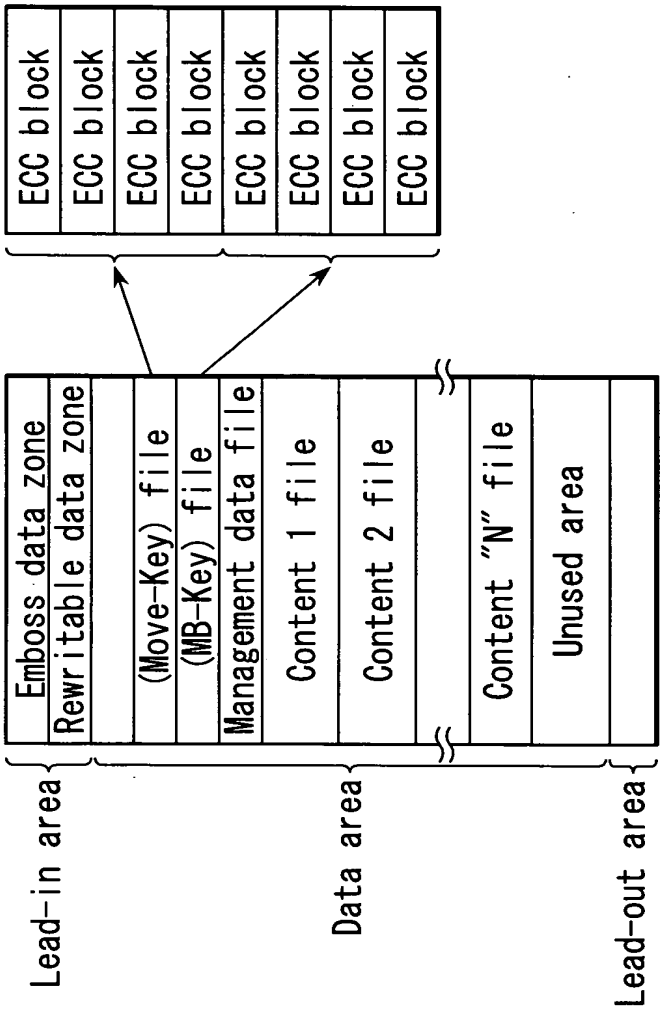
Emboss data zone
Rewritable data zone
(Move-Key) file
(MB-Key) file
Management data file
Content 1 file
Content 2 file
Content "N" file
Unused area
ECC block
Lead-in area
Data area
Lead-out area

FIG. 14

MB-Key table

File identification of encrypted encryption key (MB-Key)		
Number of CONT encrypted encryption keys		
Cont-1 Enc-TK	Cont-1 record number	○
Cont-2 Enc-TK	Cont-2 record number	○
Cont-3 Enc-TK	Cont-3 record number	×
Cont-(n-1)Enc-TK	Cont-(n-1) record number	○
Cont-n Enc-TK	Cont-n record number	○
RSB	RSB	
RSB	RSB	

(a) Information on presence or absence of Enc-2TK

Move-Key table

File identification of encrypted encryption key (Move-Key)		
Number of cont encrypted encryption keys		
Cont-1 Enc2-TK	Cont-1 record number	○
Cont-2 Enc2-TK	Cont-2 record number	○
-	Cont-3 record number	○
Cont-(n-1)Enc2-TK	Cont-(n-1) record number	○
Cont-n Enc2-TK	Cont-n record number	○
RSB	RSB	
RSB	RSB	

(b) Information on presence or absence of Enc-TK

(One table is allocated to ECC block, and each of the tables is written in quadruple in each of 4 ECC blocks.)

FIG. 15

OBLON, SPIVAK, ET AL
DOCKET # 246038US2S
INV: Tadashi KOJIMA, et al.
SHEET 14 OF 14